Security as Architecture

A fine grained multi-tiered containment strategy

Andras R. Szakal
IBM Distinguished Engineer
Chief Software Architect, U.S. Federal SWG
aszakal@us.ibm.com

SwA Forum September 2010

Objectives

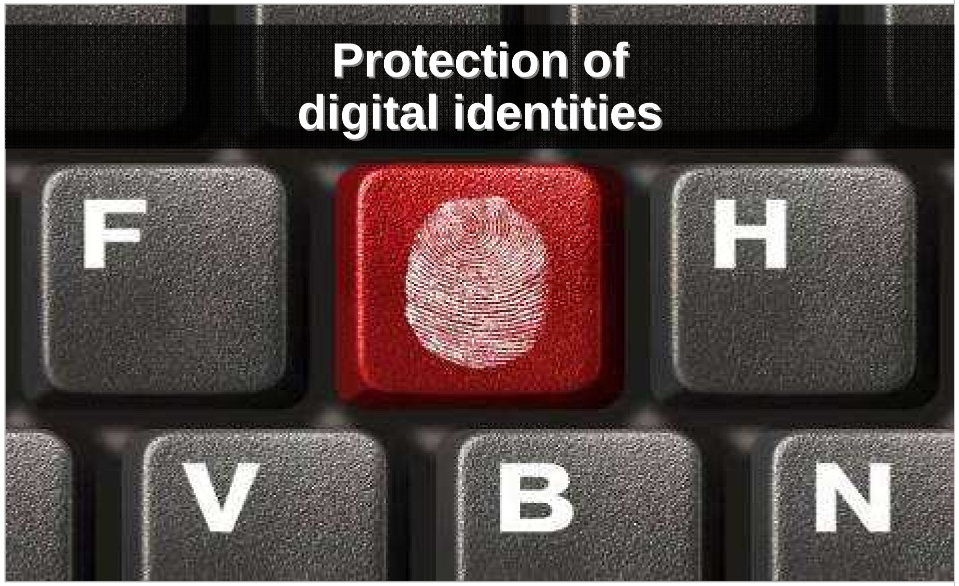
Cybersecurity - A fine grained multi-tiered containment strategy

- Defining the problem
- Multi-Tier Containment Model
- Security Patterns and Blueprints

With the smarter planet opportunities come **new security and privacy risks**

Protection of sensitive and large volumes of data, shared globally

Protection of sensors and actuators in the wild



Protection of digital identities

In order to meet risk management objectives, Smarter Planet solutions need to be Engineered for Security and Dependability.

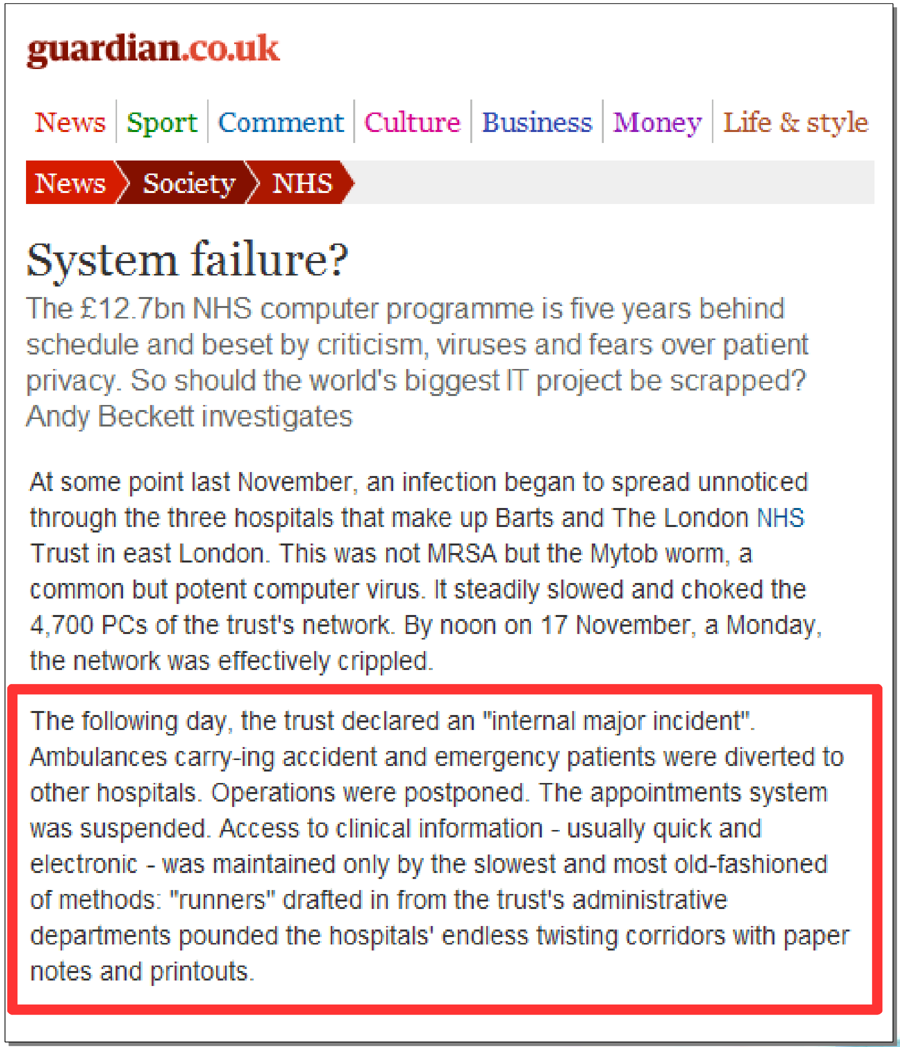
Risks & Threats
Attacking Safety
Theft of money or services
Reputational Loss
Privacy Violations
Gaming the system
Denial of Service
Subverting situational awareness
Wasting resources on false alarms
Hijacking control of equipment
Damaging assets
Physical and logical tampering

SMARTER TELECOM
Demand is skyrocketing for more and smarter ways to communicate. Can we keep up?

A smarter planet
SUSTAINABLE ENERGY
Power companies can make smarter decisions about the grid. You can make smarter decisions about your home.

SMARTER HEALTHCARE
To build a smarter system, healthcare solutions need to be instrumented, interconnected and intelligent
1976: Tonsillectomy
2001: Cervical disc disease
2008: Clavicle fracture
• Orthopedic consult
• Shoulder X-rays
• Blood calcium level

Information Technology components and systems can contribute to Infrastructure Failures & Engineering Disasters



guardian.co.uk

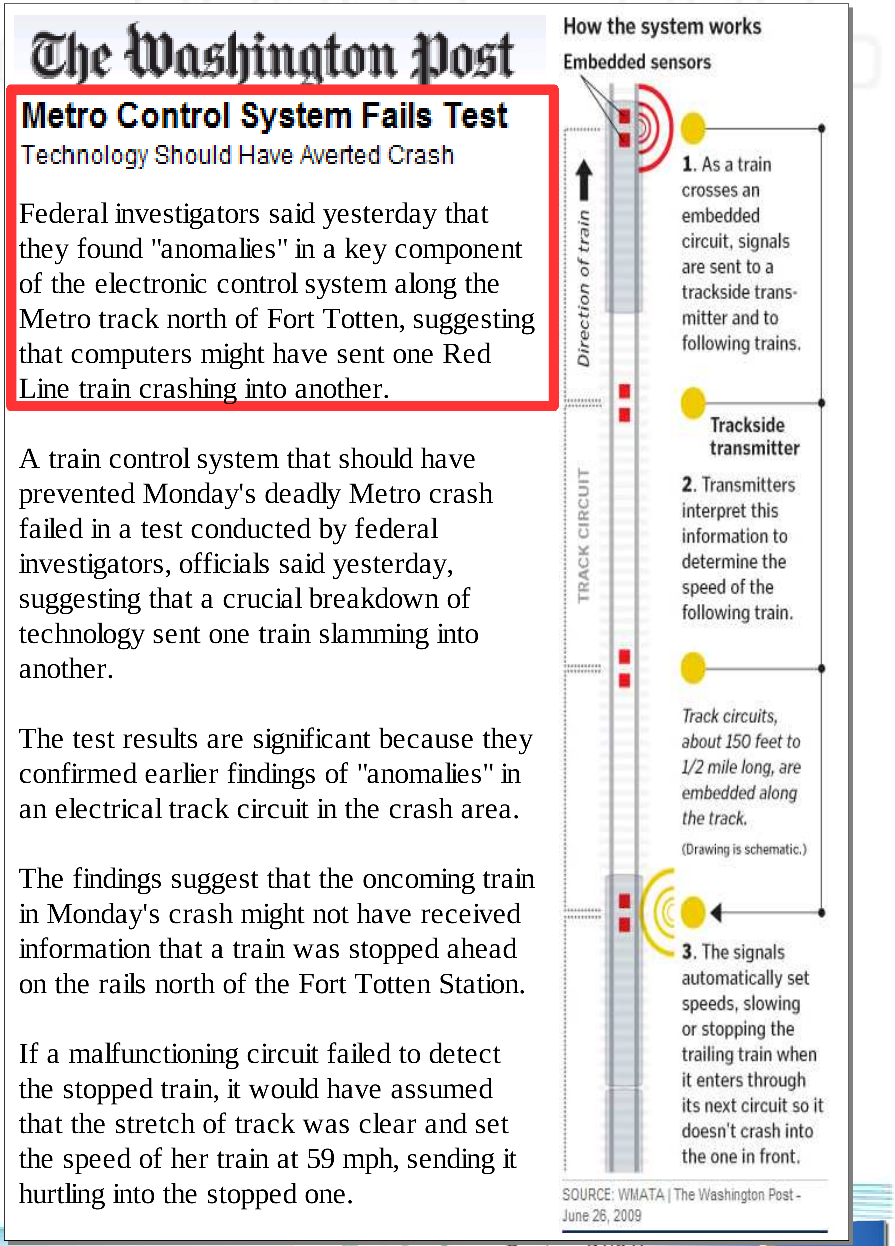
News | Sport | Comment | Culture | Business | Money | Life & style
News › Society › NHS

System failure?

The £12.7bn NHS computer programme is five years behind schedule and beset by criticism, viruses and fears over patient privacy. So should the world's biggest IT project be scrapped? Andy Beckett investigates

At some point last November, an infection began to spread unnoticed through the three hospitals that make up Barts and The London NHS Trust in east London. This was not MRSA but the Mytob worm, a common but potent computer virus. It steadily slowed and choked the 4,700 PCs of the trust's network. By noon on 17 November, a Monday, the network was effectively crippled.

The following day, the trust declared an "internal major incident". Ambulances carry-ing accident and emergency patients were diverted to other hospitals. Operations were postponed. The appointments system was suspended. Access to clinical information - usually quick and electronic - was maintained only by the slowest and most old-fashioned of methods: "runners" drafted in from the trust's administrative departments pounded the hospitals' endless twisting corridors with paper notes and printouts.



The Washington Post

Metro Control System Fails Test

Technology Should Have Averted Crash

Federal investigators said yesterday that they found "anomalies" in a key component of the electronic control system along the Metro track north of Fort Totten, suggesting that computers might have sent one Red Line train crashing into another.

A train control system that should have prevented Monday's deadly Metro crash failed in a test conducted by federal investigators, officials said yesterday, suggesting that a crucial breakdown of technology sent one train slamming into another.

The test results are significant because they confirmed earlier findings of "anomalies" in an electrical track circuit in the crash area.

The findings suggest that the oncoming train in Monday's crash might not have received information that a train was stopped ahead on the rails north of the Fort Totten Station.

If a malfunctioning circuit failed to detect the stopped train, it would have assumed that the stretch of track was clear and set the speed of her train at 59 mph, sending it hurtling into the stopped one.

How the system works

1. As a train crosses an embedded circuit, signals are sent to a trackside transmitter and to following trains.

2. Transmitters interpret this information to determine the speed of the following train.

Track circuits, about 150 feet to 1/2 mile long, are embedded along the track.

(Drawing is schematic.)

3. The signals automatically set speeds, slowing or stopping the trailing train when it enters through its next circuit so it doesn't crash into the one in front.

SOURCE: WMATA | The Washington Post - June 26, 2009

Industry Solution Requirements

Protecting a Smarter Planet

a.k.a.

Critical Infrastructure Cybersecuirty

From an IBM perspective, Cybersecurity is the practice of achieving the resilience of a Smarter Planet

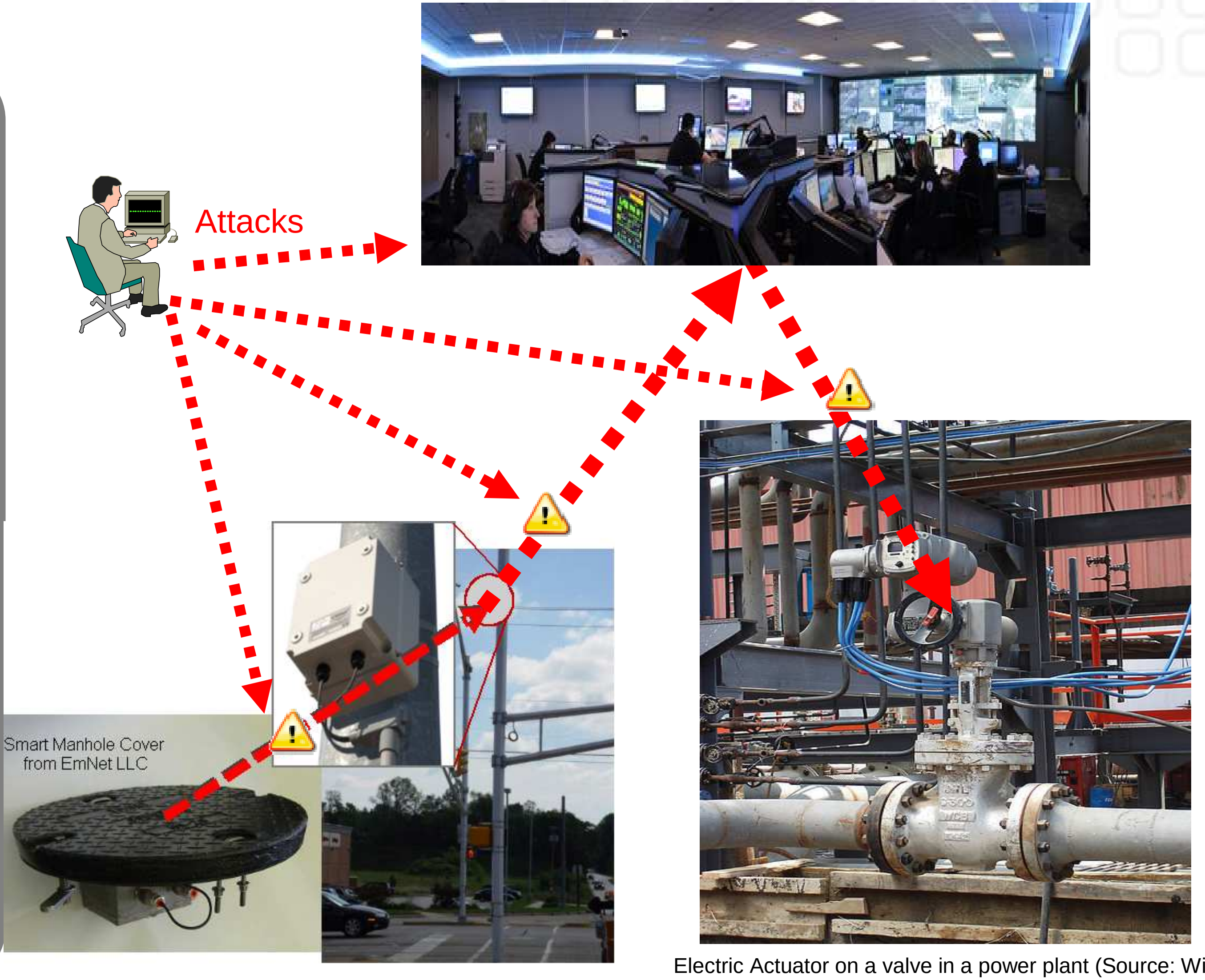
Case Study: Sensors and Actuators in the Wild

Sensors and Actuators In The Wild

Driver:
Smarter Planet Industries make high-value decisions based on information that originates from “sensors in the wild.”

Challenge: ⚠
Sensors are not sufficiently physically secure and sensor data is not sufficiently protected from attack relative to the high value decisions that are made based on them.

The link between the points of data acquisition and the point of data processing is often broken.



Electric Actuator on a valve in a power plant (Source: Wikipedia)

What Are We Concerned About?

Human Accountability

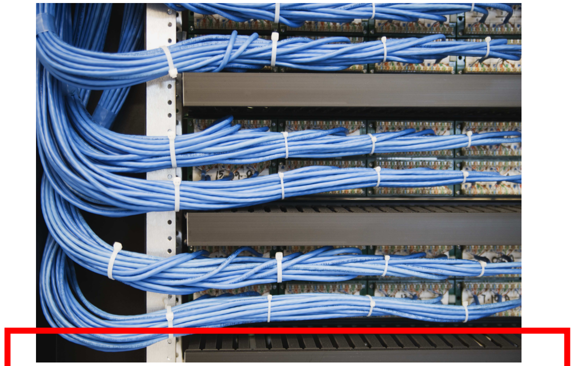
People

Society

Privacy

Compliance

Biometrics



{Netcentric Technology}

High-Impact Processes

Physical Location

Physical Objects

Nature

Real-time Processes

Physical Identities

Physical Data

Autonomous Control

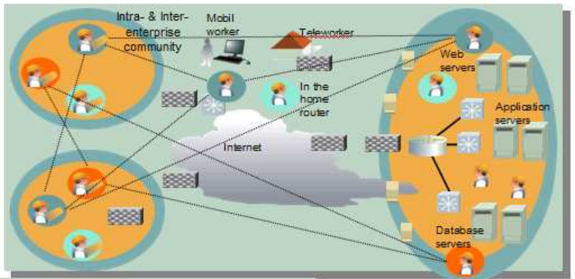
Legacy of Vulnerable Process Control Technology

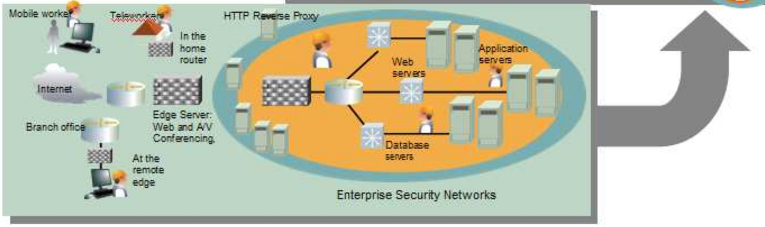
Physical Sensors

"in the wild"

Physical Actuators

Multi-Tier Architecture & Deperimeterization



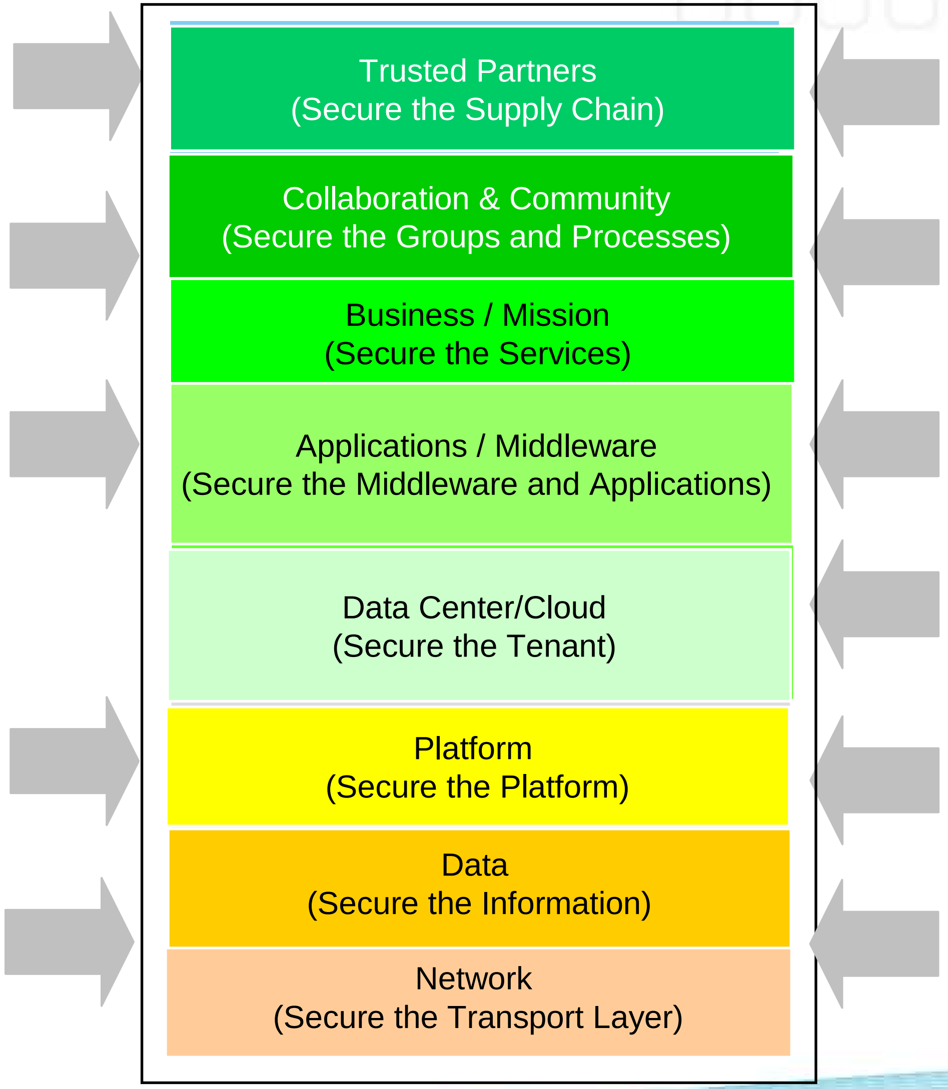


Multi-Tier Architecture - Our architectures have become componentized, service-based and distributed across platforms and service providers.

We no longer have control over all our high value assets we have become **deperimeterized.**

Fine-Grained Multi-Tier Containment

- Supplier Integiry
- Identity Management
- Collaboration - Gov to Gov; Gov to Industry; Gov the Critical infrastructure; Industry to Industry (ICT)
- Information Assurance
- Smart Information Environments
- Data Protection throughout the life-cycle
- Defending Networks and gateways
- Persistent threat issues
- Continuous Network Monitoring
- High Performance Computing



Trusted Partners
(Secure the Supply Chain)

Collaboration & Community
(Secure the Groups and Processes)

Business / Mission
(Secure the Services)

Applications / Middleware
(Secure the Middleware and Applications)

Data Center/Cloud
(Secure the Tenant)

Platform
(Secure the Platform)

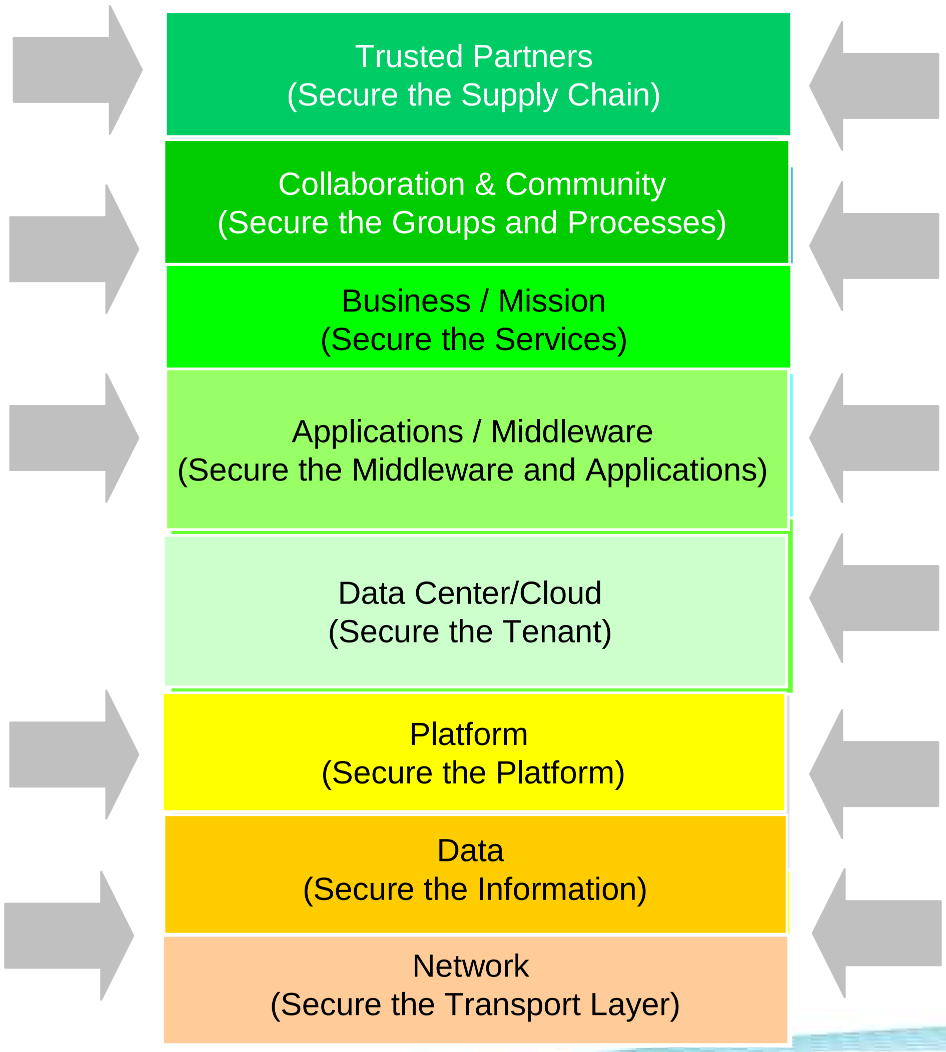
Data
(Secure the Information)

Network
(Secure the Transport Layer)

- Compliance - validation of policies (IT)
- Situational Awareness of the Government ecosystems
- Central Operations Center - government sensitive, civilian agencies/dept, CIP and industry
- IoD / Analytics
- Analytics / Dashboarding

Fine-Grained Multi-Tier Containment

- Identity Management
- Collaboration - Gov to Gov; Gov to Industry; Gov the Critical infrastructure; Industry to Industry (ICT)
- Information Assurance
- Smart Information Environments
- Data Protection throughout the life-cycle
- Defending Networks and gateways
- Persistent threat issues
- Supply Chain
- High Performance Computing



Trusted Partners
(Secure the Supply Chain)

Collaboration & Community
(Secure the Groups and Processes)

Business / Mission
(Secure the Services)

Applications / Middleware
(Secure the Middleware and Applications)

Data Center/Cloud
(Secure the Tenant)

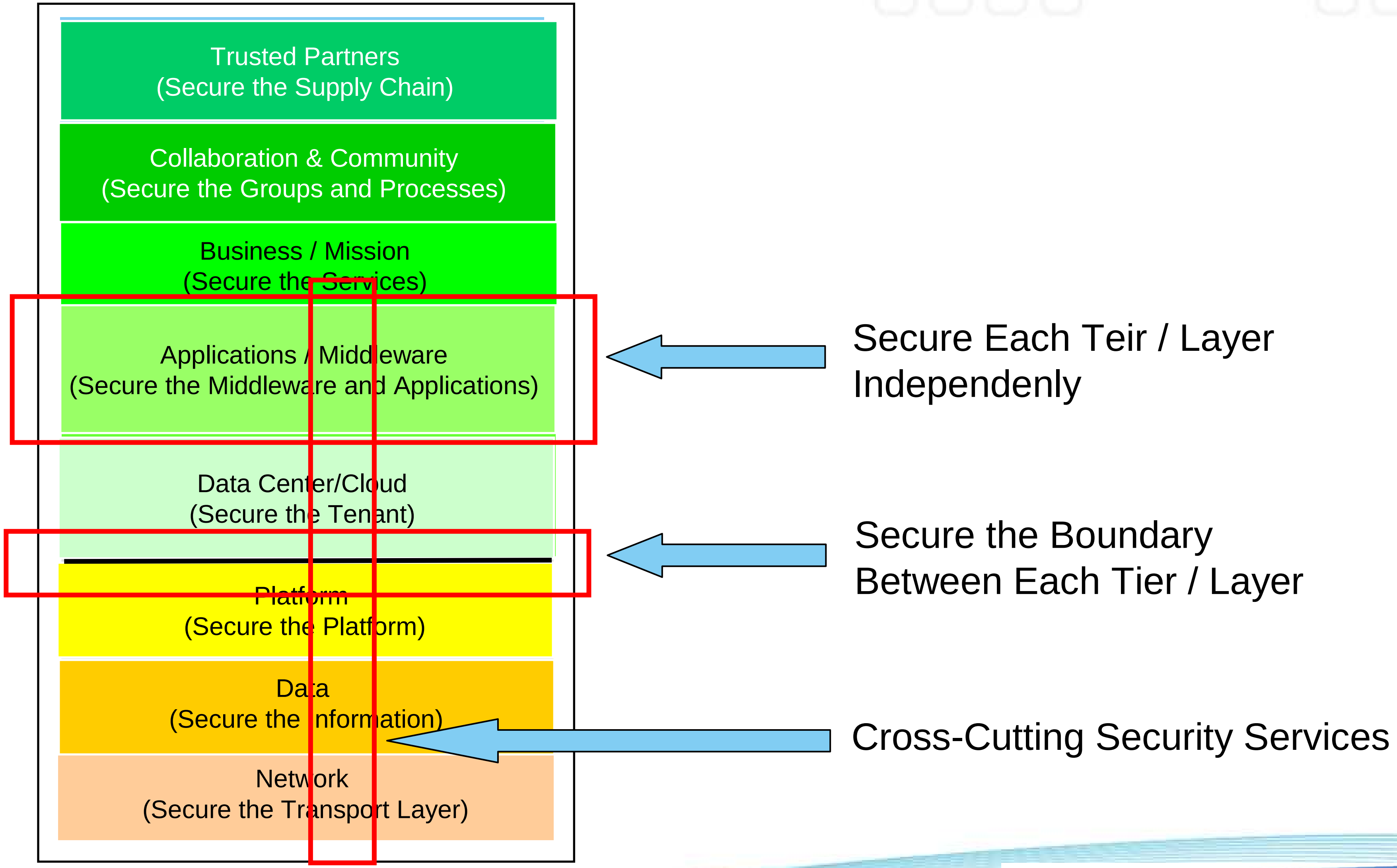
Platform
(Secure the Platform)

Data
(Secure the Information)

Network
(Secure the Transport Layer)

- Compliance - validation of policies (IT)
- Situational Awareness of the Government ecosystems
- Central Operations Center - government sensitive, civilian agencies/dept, CIP and industry
- IoD / Analytics
- Analytics / Dashboarding

Multi-Tier Containment Strategy



Trusted Partners
(Secure the Supply Chain)

Collaboration & Community
(Secure the Groups and Processes)

Business / Mission
(Secure the Services)

Applications / Middleware
(Secure the Middleware and Applications)

Data Center/Cloud
(Secure the Tenant)

Platform
(Secure the Platform)

Data
(Secure the Information)

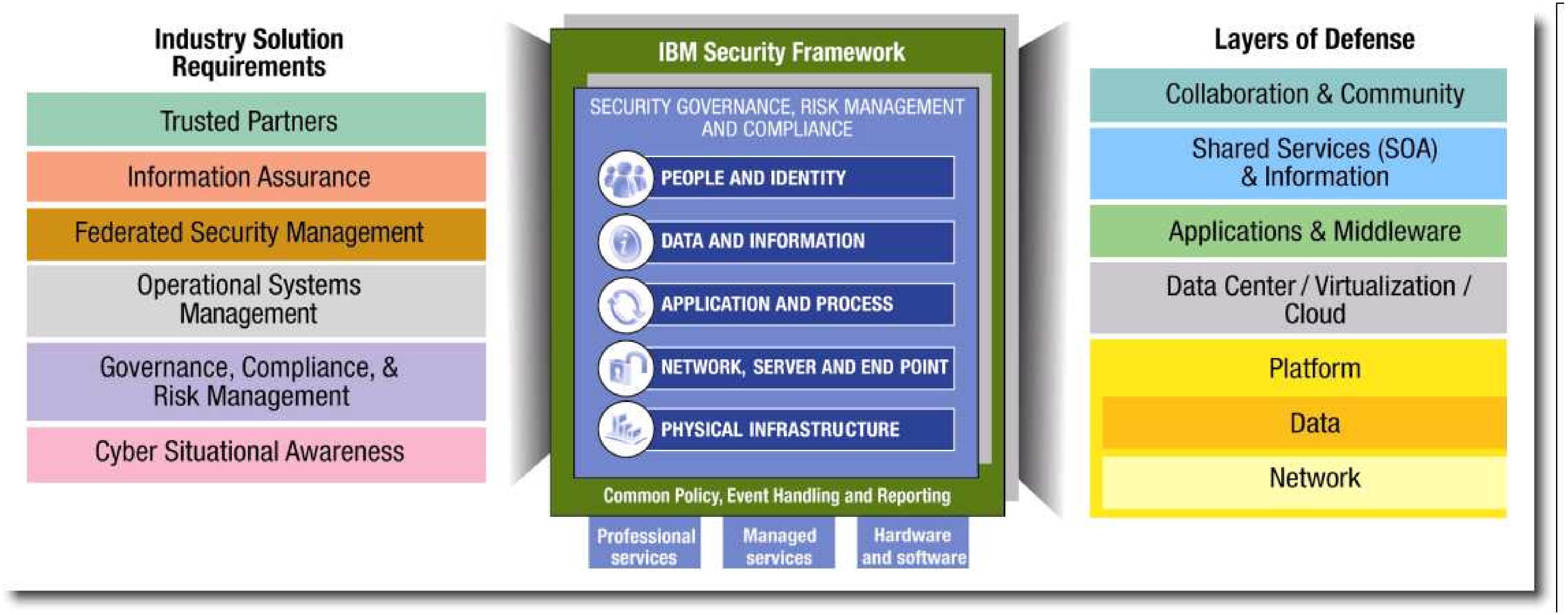
Network
(Secure the Transport Layer)

Secure Each Teir / Layer Independenly

Secure the Boundary Between Each Tier / Layer

Cross-Cutting Security Services

Cybersecurity Model
Based on the IBM Security Framework



Industry Solution Requirements

- Trusted Partners
- Information Assurance
- Federated Security Management
- Operational Systems Management
- Governance, Compliance, & Risk Management
- Cyber Situational Awareness

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

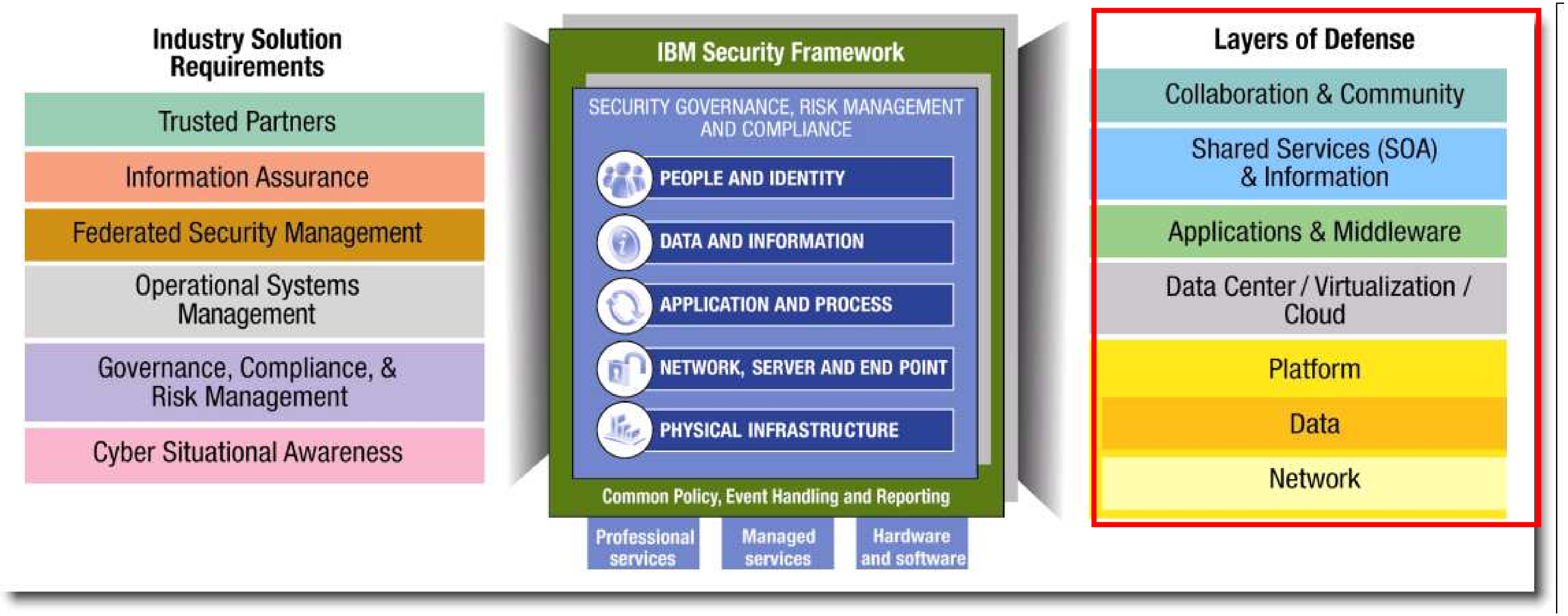
- Professional services
- Managed services
- Hardware and software

Layers of Defense

- Collaboration & Community
- Shared Services (SOA) & Information
- Applications & Middleware
- Data Center / Virtualization / Cloud
- Platform
- Data
- Network

Fine-Grained Multi-Tier Containment

Cybersecurity Model
Foundational Security Components



Industry Solution Requirements

- Trusted Partners
- Information Assurance
- Federated Security Management
- Operational Systems Management
- Governance, Compliance, & Risk Management
- Cyber Situational Awareness

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services | Managed services | Hardware and software

Layers of Defense

- Collaboration & Community
- Shared Services (SOA) & Information
- Applications & Middleware
- Data Center / Virtualization / Cloud
- Platform
- Data
- Network

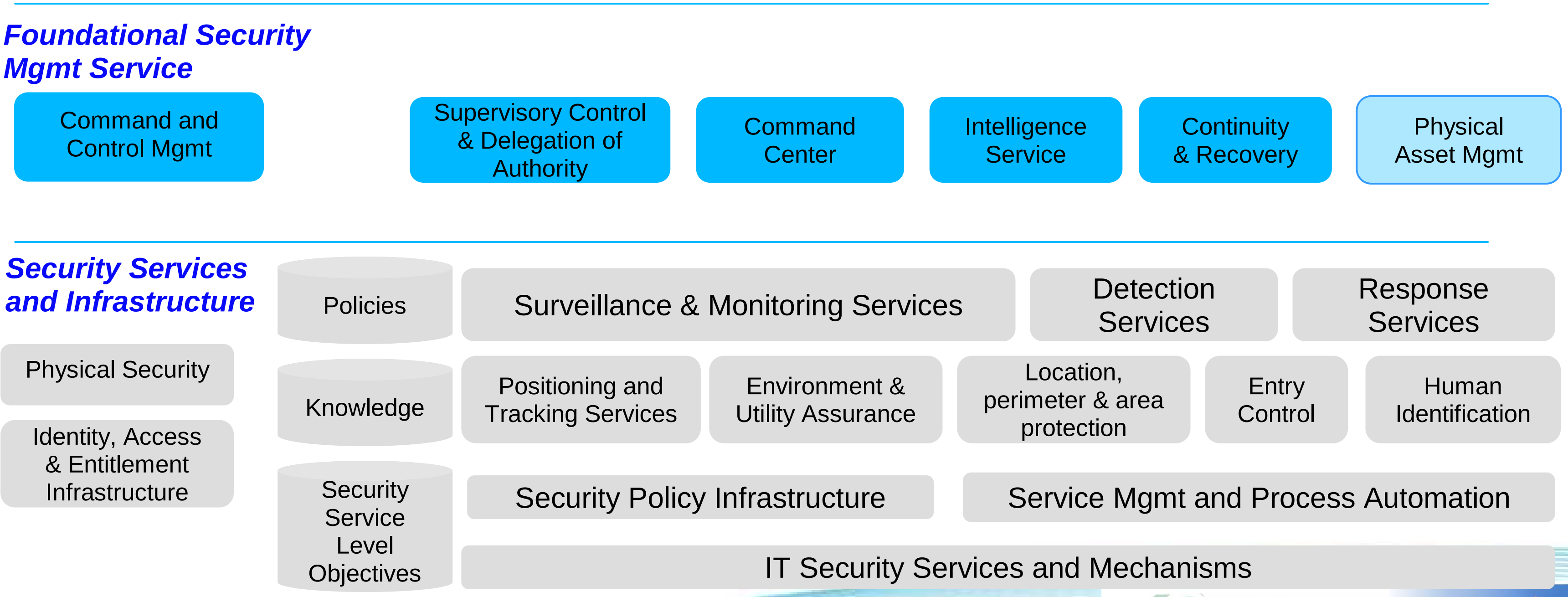
Foundational Security Management

- Software, System & Service Assurance
- Identity, Access & Entitlement Mgmt
- Data & Information Protection Mgmt
- Threat & Vulnerability Management
- IT Service Management
- Command and Control Mgmt
- Security Policy Management
- Risk & Compliance Assessment
- Physical Asset Management

Secure the Platform (Operating Environment)

Focus: Command and Control Management provides the command center for security management as well as the operational security capabilities for non-IT assets and services to ensure protection, response, continuity and recovery**.**

Includes: Providing the approving authority for security; ensuring that physical and operational security is maintained for locations, assets, humans, environment and utilities; providing surveillance and monitoring of locations, perimeters and areas; enforce entry controls; providing for positioning, tracking and identification of humans and assets; continuity and recovery operations.



Foundational Security Mgmt Service

Command and Control Mgmt

Supervisory Control & Delegation of Authority

Command Center

Intelligence Service

Continuity & Recovery

Physical Asset Mgmt

Security Services and Infrastructure

Physical Security

Identity, Access & Entitlement Infrastructure

Policies

Knowledge

Security Service Level Objectives

Surveillance & Monitoring Services

Detection Services

Response Services

Positioning and Tracking Services

Environment & Utility Assurance

Location, perimeter & area protection

Entry Control

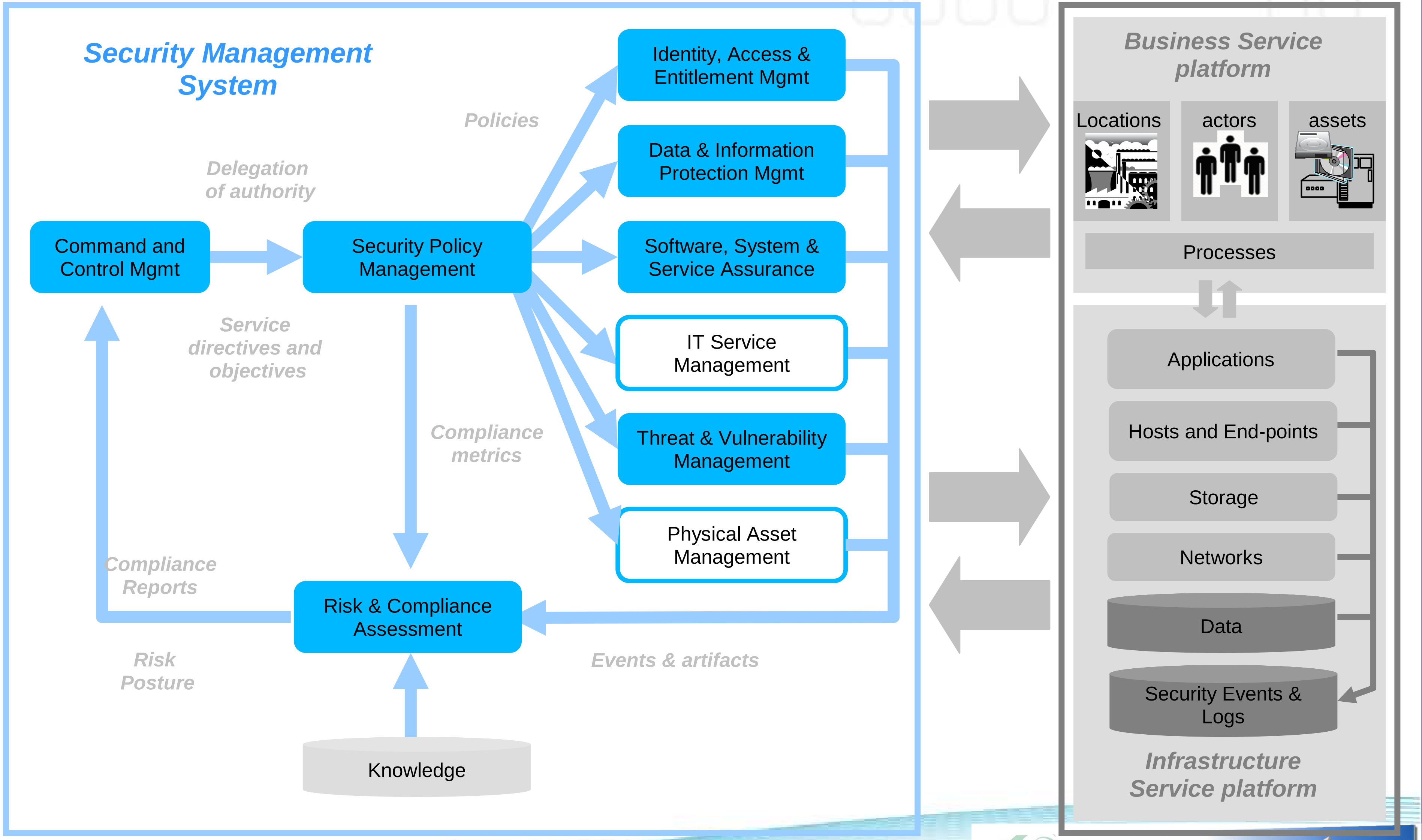
Human Identification

Security Policy Infrastructure

Service Mgmt and Process Automation

IT Security Services and Mechanisms

Secure the Platform – Architectural Pattern



Security Management System

Command and Control Mgmt

Delegation of authority

Security Policy Management

Policies

Identity, Access & Entitlement Mgmt

Data & Information Protection Mgmt

Software, System & Service Assurance

IT Service Management

Threat & Vulnerability Management

Physical Asset Management

Service directives and objectives

Compliance metrics

Compliance Reports

Risk & Compliance Assessment

Events & artifacts

Risk Posture

Knowledge

Business Service platform

Locations

actors

assets

Processes

Applications

Hosts and End-points

Storage

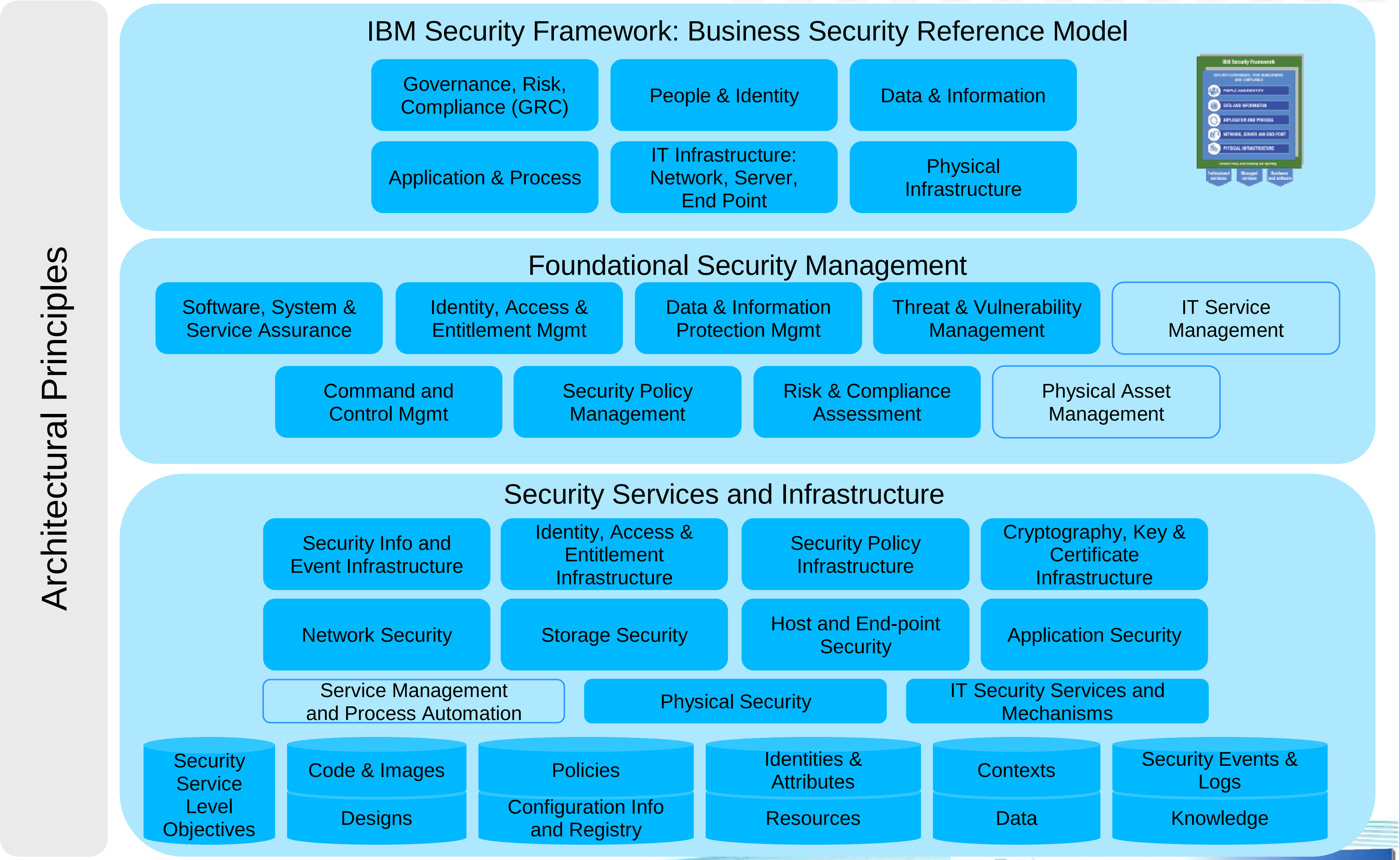
Networks

Data

Security Events & Logs

Infrastructure Service platform

Security Blueprint Patterns



Architectural Principles

IBM Security Framework: Business Security Reference Model

- Governance, Risk, Compliance (GRC)
- People & Identity
- Data & Information
- Application & Process
- IT Infrastructure: Network, Server, End Point
- Physical Infrastructure

Foundational Security Management

- Software, System & Service Assurance
- Identity, Access & Entitlement Mgmt
- Data & Information Protection Mgmt
- Threat & Vulnerability Management
- IT Service Management
- Command and Control Mgmt
- Security Policy Management
- Risk & Compliance Assessment
- Physical Asset Management

Security Services and Infrastructure

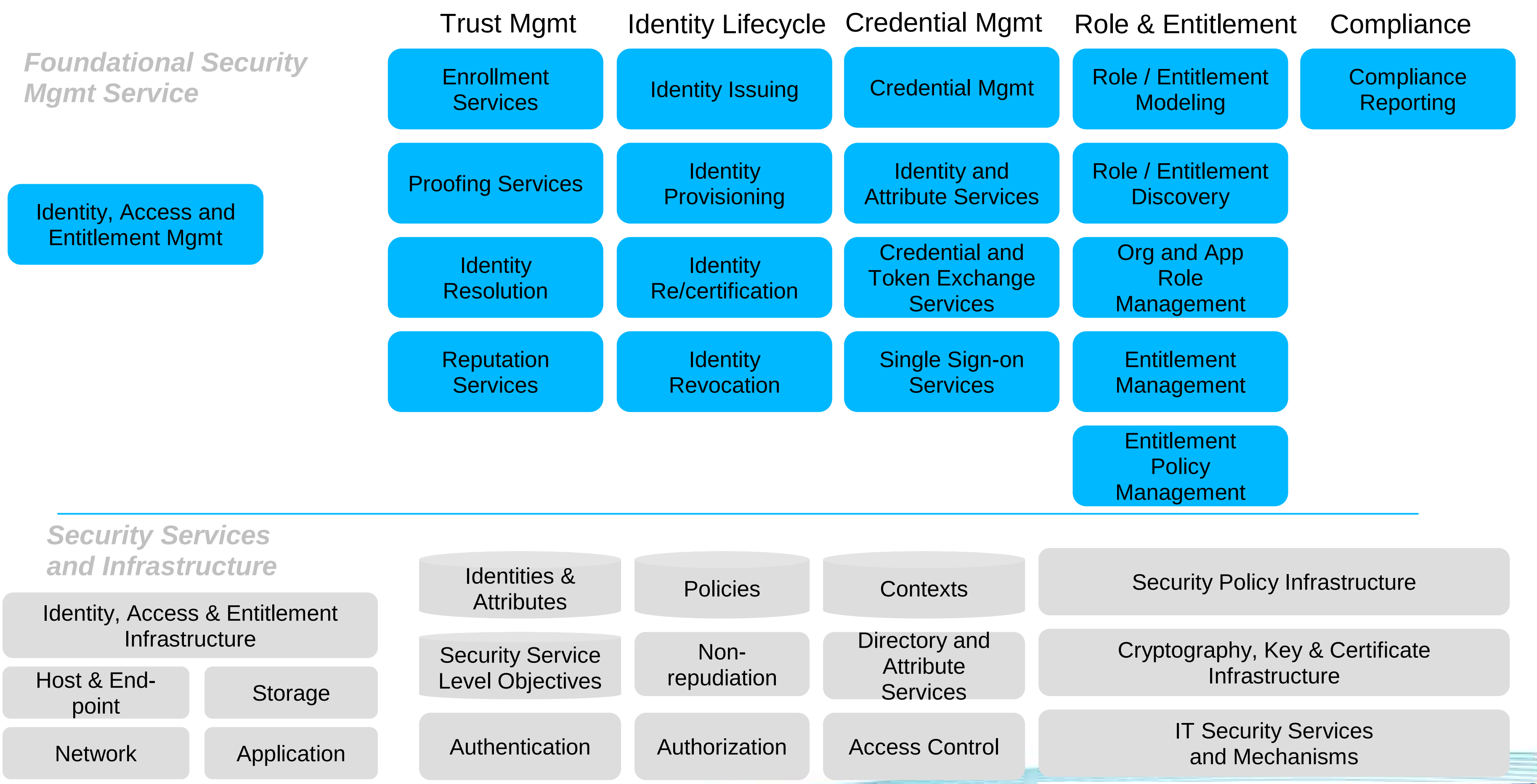
- Security Info and Event Infrastructure
- Identity, Access & Entitlement Infrastructure
- Security Policy Infrastructure
- Cryptography, Key & Certificate Infrastructure
- Network Security
- Storage Security
- Host and End-point Security
- Application Security
- Service Management and Process Automation
- Physical Security
- IT Security Services and Mechanisms
- Security Service Level Objectives
- Code & Images
- Designs
- Policies
- Configuration Info and Registry
- Identities & Attributes
- Resources
- Contexts
- Data
- Security Events & Logs
- Knowledge

Thank you!

For more information, please visit:
ibm.com/cloud
Ibm.com/security

Identity, Access & Entitlement Management

Focus: This sublayer provides all services related to roles and identities, access rights and entitlements. The goal of these services is to assure that access to resources has been given to the right identities, at the right time, for the right purpose. It also supports that access to resources is monitored and audited for unauthorized or unacceptable use.



Foundational Security Mgmt Service

Identity, Access and Entitlement Mgmt

Trust Mgmt	Identity Lifecycle	Credential Mgmt	Role & Entitlement	Compliance
Enrollment Services	Identity Issuing	Credential Mgmt	Role / Entitlement Modeling	Compliance Reporting
Proofing Services	Identity Provisioning	Identity and Attribute Services	Role / Entitlement Discovery	
Identity Resolution	Identity Re/certification	Credential and Token Exchange Services	Org and App Role Management	
Reputation Services	Identity Revocation	Single Sign-on Services	Entitlement Management	
			Entitlement Policy Management	

Security Services and Infrastructure

- Identity, Access & Entitlement Infrastructure
- Host & End-point
- Storage
- Network
- Application

Identities & Attributes	Policies	Contexts	Security Policy Infrastructure
Security Service Level Objectives	Non-repudiation	Directory and Attribute Services	Cryptography, Key & Certificate Infrastructure
Authentication	Authorization	Access Control	IT Security Services and Mechanisms

The Open Group Boston 2010
Hyatt Harborside
Boston, Massachusetts, USA
July 19-23, 2010

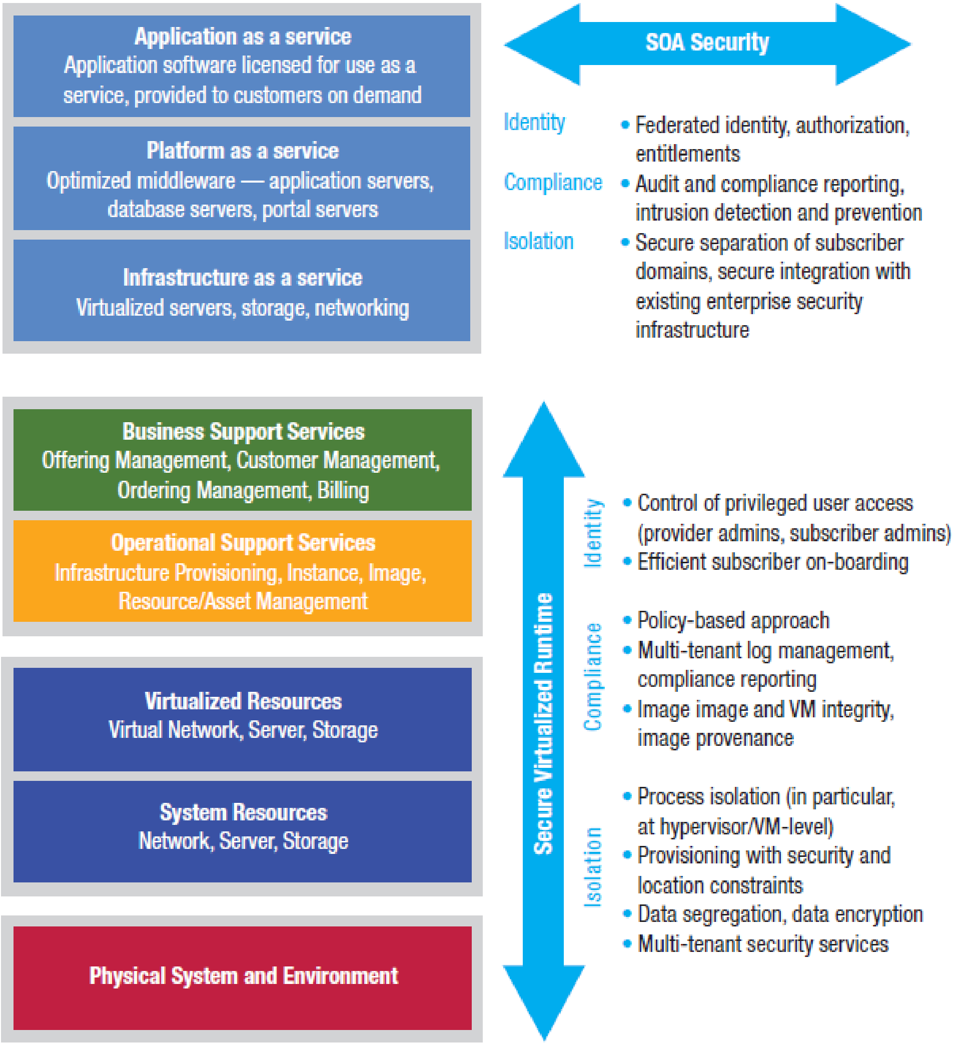
IBM

Trusted Advisor | Solution Provider | Security Company | The Company

Security for the Cloud | **Security from the Cloud**

Security & Privacy Leadership

Cloud Security = SOA Security + Secure Virtualized Runtime



Application as a service
Application software licensed for use as a service, provided to customers on demand

Platform as a service
Optimized middleware — application servers, database servers, portal servers

Infrastructure as a service
Virtualized servers, storage, networking

SOA Security

Identity
- Federated identity, authorization, entitlements

Compliance
- Audit and compliance reporting, intrusion detection and prevention

Isolation
- Secure separation of subscriber domains, secure integration with existing enterprise security infrastructure

Business Support Services
Offering Management, Customer Management, Ordering Management, Billing

Operational Support Services
Infrastructure Provisioning, Instance, Image, Resource/Asset Management

Virtualized Resources
Virtual Network, Server, Storage

System Resources
Network, Server, Storage

Physical System and Environment

Secure Virtualized Runtime

Identity
- Control of privileged user access (provider admins, subscriber admins)
- Efficient subscriber on-boarding

Compliance
- Policy-based approach
- Multi-tenant log management, compliance reporting
- Image image and VM integrity, image provenance

Isolation
- Process isolation (in particular, at hypervisor/VM-level)
- Provisioning with security and location constraints
- Data segregation, data encryption
- Multi-tenant security services

Two examples:

IBM Tivoli Federated Identity Manager

IBM Security Virtual Server Protection

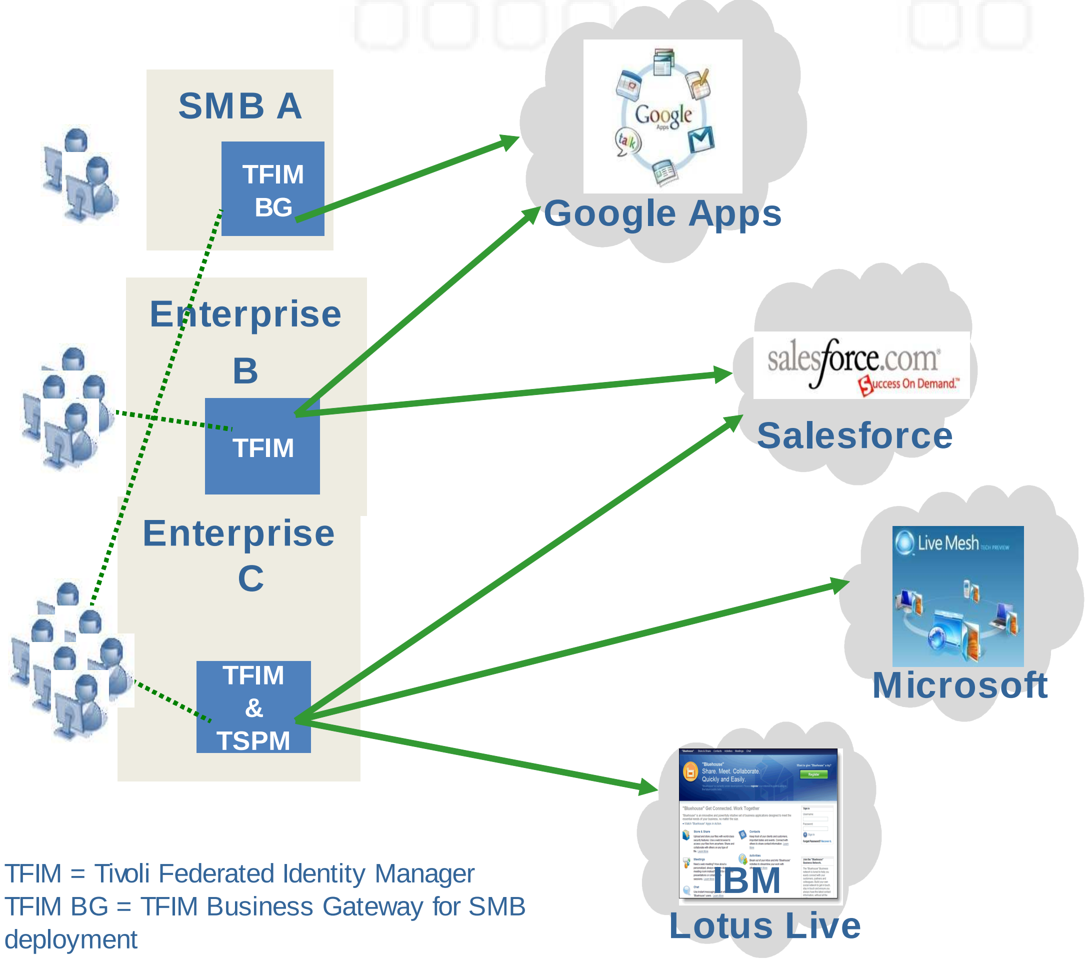
Example 1: IBM Tivoli Federated Identity Manager

- Centralized user access management to on- and off-premise apps and services

- Wide variety of Federated SSO protocols
- SAML 1.0 / 1.1 / 2.0
- WS-Federation
- Liberty ID-FF 1.1/ 1.2
- Information Card Profile 1.0
- OpenID
- Integration with IBM LotusLive, Google Apps, salesforce.com, etc.

- Tools for user enrollment, WS-Trust based security token services, web access management

- Simplify integration across Java, .NET and mainframe environments

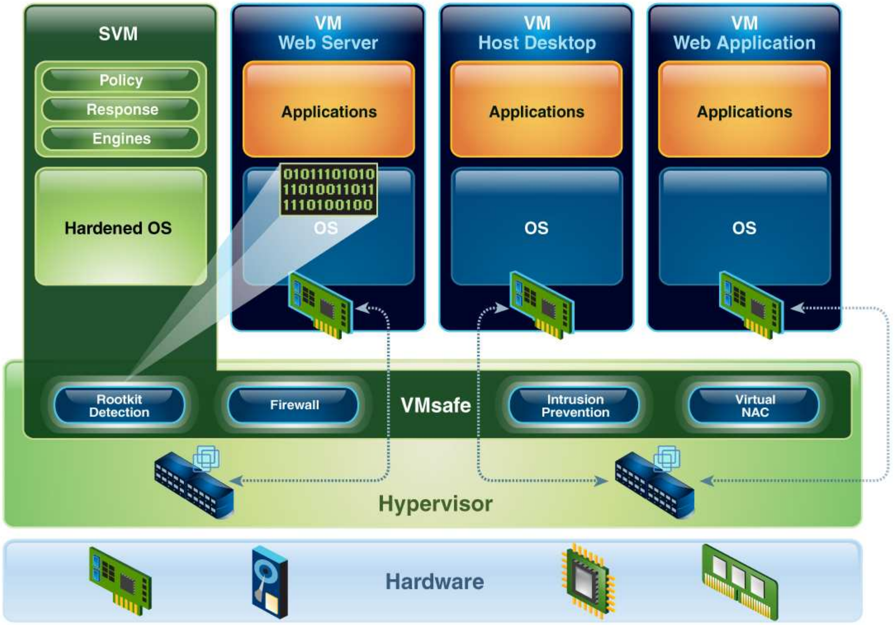


TFIM = Tivoli Federated Identity Manager
TFIM BG = TFIM Business Gateway for SMB deployment
TSPM = Tivoli Security Policy Manager for data entitlement management

Example 2: IBM Security Virtual Server Protection for VMware

Integrated threat protection for VMware vSphere 4

Offers broadest, most integrated, defense-in-depth virtualization security with *one product*

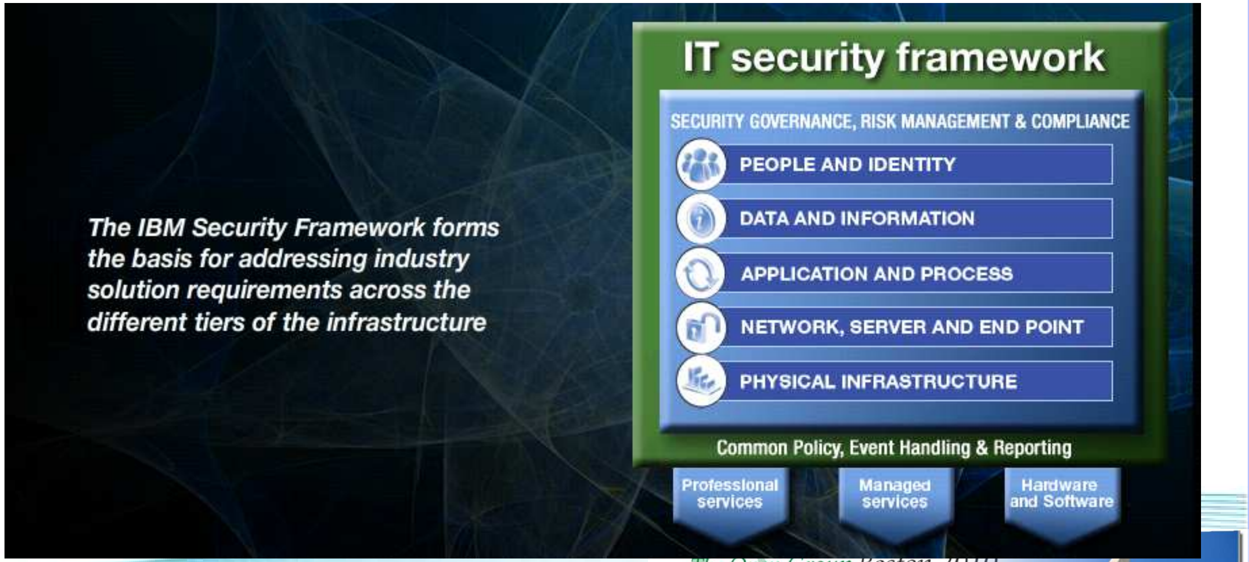


- Provides dynamic protection for every layer of the virtual infrastructure
- Helps meet regulatory compliance by providing security and reporting functionality customized for the virtual infrastructure
- Increases ROI of the virtual infrastructure with easy to maintain, easy to deploy security

- Firewall
- VMsafe Integration
- Rootkit Detection
- Intrusion Detection & Prevention
- Inter-VM Traffic Analysis
- VM Sprawl Management
- Network Policy Enforcement
- Automated Protection for Mobile VMs (VMotion)

- Auto Discovery
- Virtual Infrastructure Auditing (Privileged User Access)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Network Access Control
- Central Management
- Web Application Protection
- Virtual Patch

Deperimeterization & IBM Security Framework



The IBM Security Framework forms the basis for addressing industry solution requirements across the different tiers of the infrastructure

IT security framework

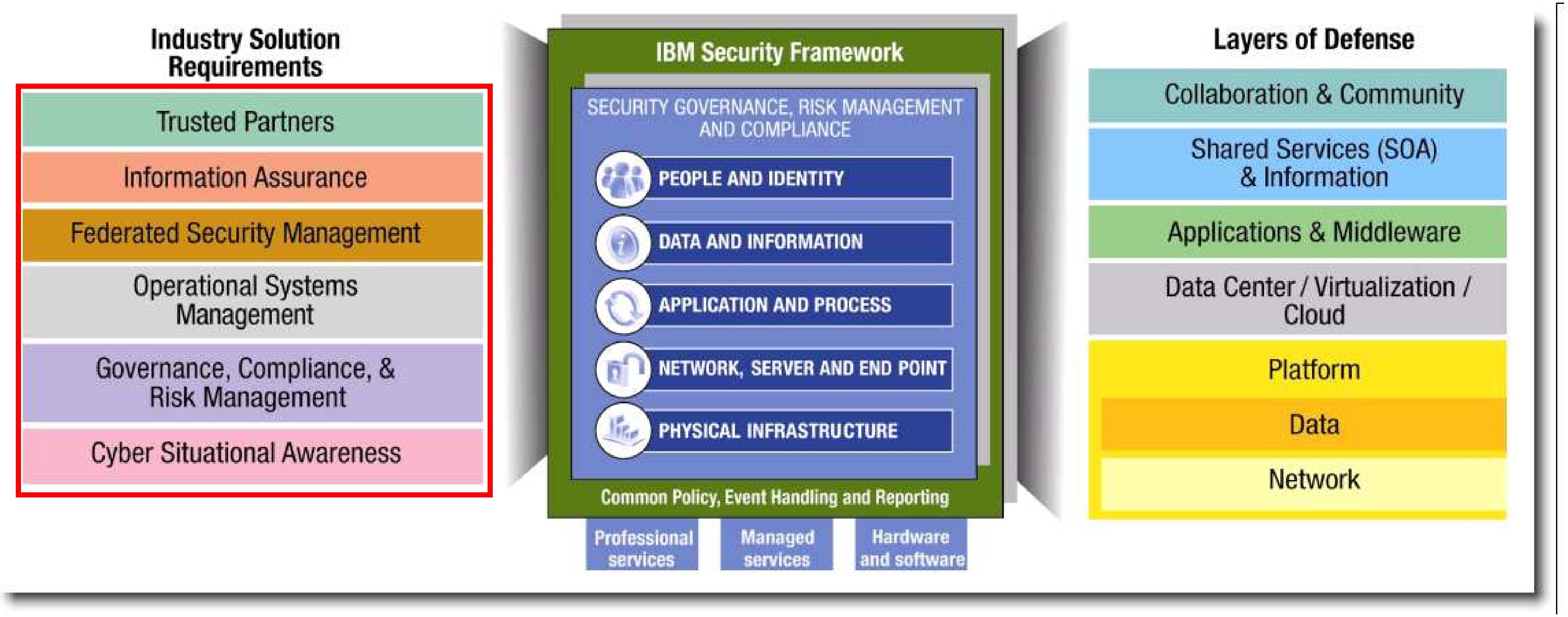
SECURITY GOVERNANCE, RISK MANAGEMENT & COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling & Reporting

Professional services | Managed services | Hardware and Software

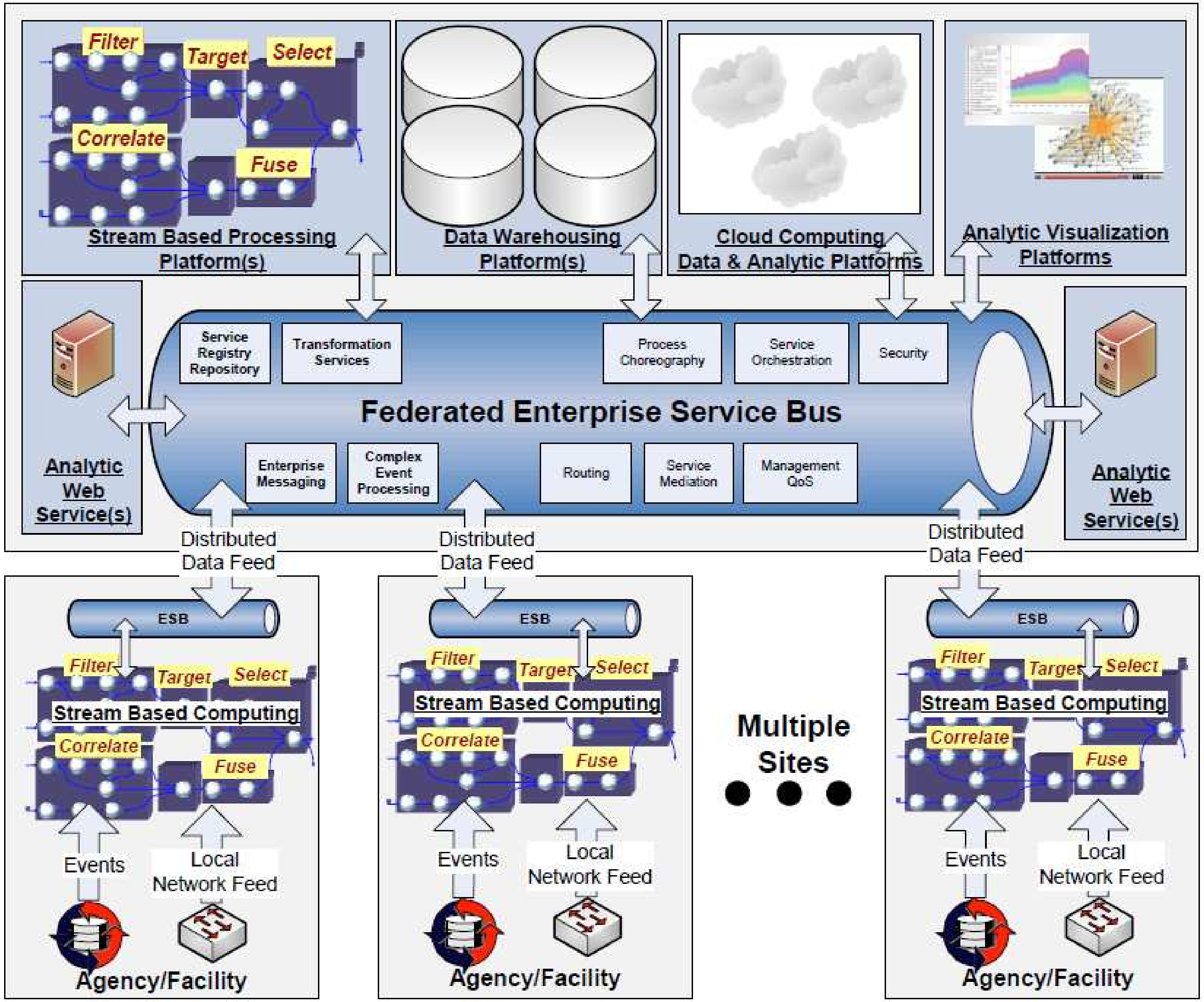
Cybersecurity Model
Based on the IBM Security Framework


Industry Solution Requirements
Trusted Partners
Information Assurance
Federated Security Management
Operational Systems Management
Governance, Compliance, & Risk Management
Cyber Situational Awareness
IBM Security Framework
SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE
PEOPLE AND IDENTITY
DATA AND INFORMATION
APPLICATION AND PROCESS
NETWORK, SERVER AND END POINT
PHYSICAL INFRASTRUCTURE
Common Policy, Event Handling and Reporting
Professional services
Managed services
Hardware and software
Layers of Defense
Collaboration & Community
Shared Services (SOA) & Information
Applications & Middleware
Data Center / Virtualization / Cloud
Platform
Data
Network

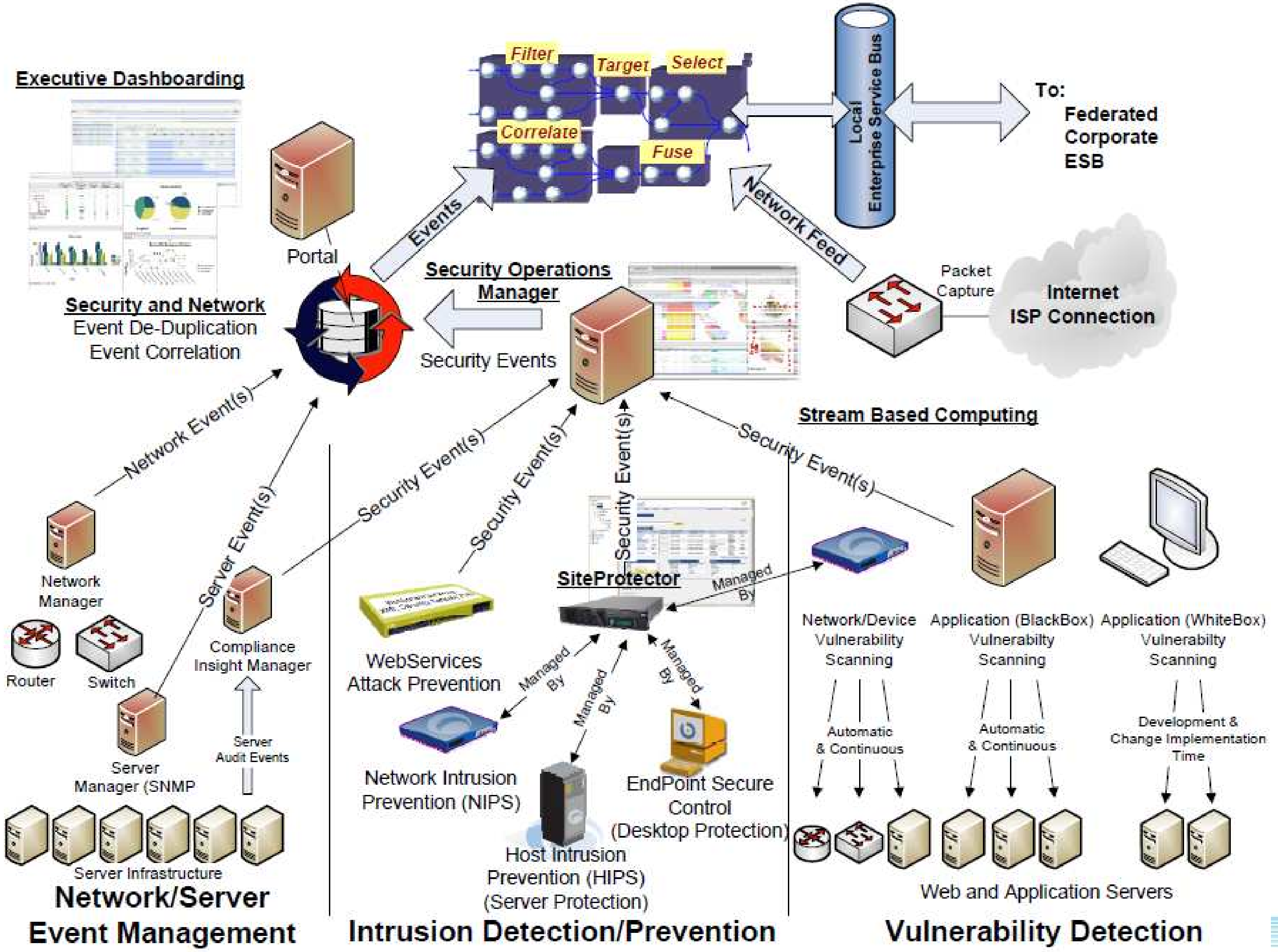
Cyber security Solution Requirements

Cybersecurity - Situational Awareness

- Full spectrum analysis of security relevant events:
  - Network
  - Application
  - Platform
  - Data
  - Behavioral
- Integrated Command and Control



Cyber Security Architectural Overview



SwA Forum September 2010

The Open Group Boston 2010
Hyatt Harborside
Boston, Massachusetts, USA
July 19-23, 2010

IBM Secure Engineering Framework

- Published the IBM Secure Engineering Framework
- Represents a compilation of internal security practices
- Provides consistent mes
- Differentiates IBM capab
- Can provide a unified go development tools

Common
Development Process

Supply
ain Security

Provide structure, execution and accountability for software and solution development projects

uild and Maintain trusted ationships with suppliers, tribution channels, import/ port and customer support

Best so de

of s

IBM

Draft Document for Review February 2, 2010 6:45 pm

REDP-4641-00

Security in Development: The IBM Secure Engineering Framework

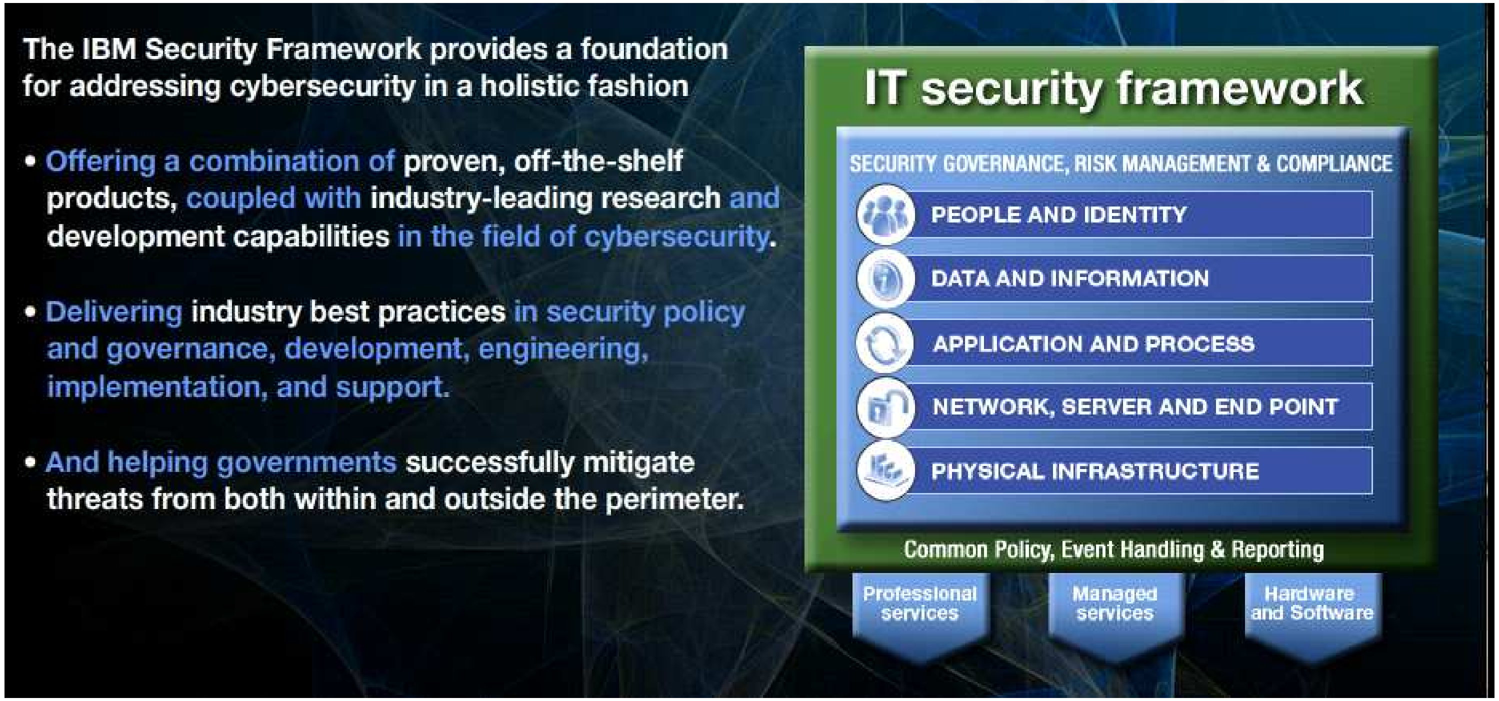
Redguides
for Business Leaders

Danny Allan
Tim Hahn
Andras Szakal
Jim Whitmore
Axel Buecker

- Investigating common development processes and the IBM Integrated Product Development process
- Emphasizing security awareness and requirements in the software development process
- Discussing test and vulnerability assessments

Redbooks

IBM’s Holistic Cyber Security Approach



The IBM Security Framework provides a foundation for addressing cybersecurity in a holistic fashion

- Offering a combination of proven, off-the-shelf products, coupled with industry-leading research and development capabilities in the field of cybersecurity.
- Delivering industry best practices in security policy and governance, development, engineering, implementation, and support.
- And helping governments successfully mitigate threats from both within and outside the perimeter.

IT security framework

SECURITY GOVERNANCE, RISK MANAGEMENT & COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling & Reporting

- Professional services
- Managed services
- Hardware and Software

IBM security framework podcasts @ the IBM Institute for Advanced Security

http://www-304.ibm.com/industries/publicsector/us/en/rep/!!/xmlid=192485

IBM Institute for Advanced Security
Enabling cybersecurity innovation and collaboration